



## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2001265771 A**(43) Date of publication of application: **28.09.01**

(51) Int. Cl.

**G06F 17/30**  
**G06F 12/14**  
**G06F 17/60**

(21) Application number: **2000079411**(22) Date of filing: **22.03.00**(71) Applicant: **NIPPON TELEGR & TELEPH  
CORP <NTT>**(72) Inventor: **YAMAMOTO KANA  
HORIOKA TSUTOMU  
TAKASHIMA YOICHI**

(54) **DEVICE AND METHOD FOR MANAGING  
PERSONAL INFORMATION AND RECORDING  
MEDIUM RECORDING PROGRAM FOR  
EXECUTING THE DEVICE OR METHOD**

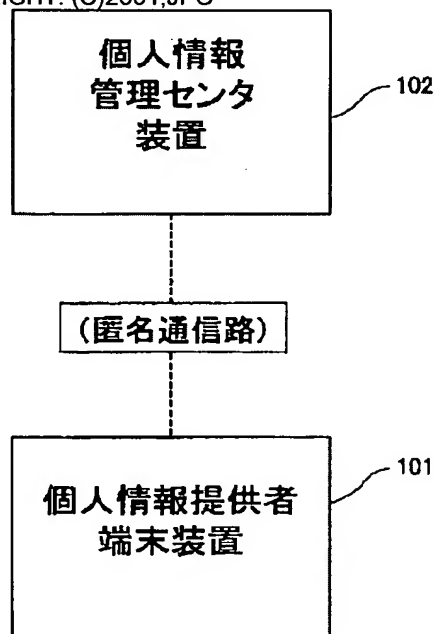
and only in the case of matching to the acquisition  
agreement conditions, personal information is provided.

COPYRIGHT: (C)2001,JPO

(57) Abstract:

**PROBLEM TO BE SOLVED:** To solve the problem that is a hand to protect privacy and there is the danger of leak to a third person in personal information provision on a network through a managing center.

**SOLUTION:** Personal information on personal information provider terminal equipment 101 to provide personal information to the other person is registered in a personal information managing center device 102 after being divided into partial personal information, which can not be related with a specified individual respectively singly and is meaningless, and by holding the relation of such information only on the terminal of a personal information provider, the privacy of the personal information provider can not be grasped in the personal information managing center. Besides, the set of the identifier of the partial personal information registered in the personal information managing center and personal information acquisition agreement conditions is provided to a personal information user



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-265771

(P2001-265771A)

(43) 公開日 平成13年9月28日 (2001.9.28)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テマート* (参考)
G 0 6 F 17/30	1 2 0	G 0 6 F 17/30	1 2 0 A 5 B 0 1 7
	1 7 0		1 7 0 Z 5 B 0 4 9
	3 4 0		3 4 0 A 5 B 0 7 5
12/14	3 2 0	12/14	3 2 0 B
17/60	1 7 2	17/60	1 7 2
審査請求 未請求 請求項の数22 O L (全 24 頁) 最終頁に続く			

(21) 出願番号 特願2000-79411(P2000-79411)

(22) 出願日 平成12年3月22日 (2000.3.22)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 山本 奏

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(72) 発明者 堀岡 力

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(74) 代理人 100062199

弁理士 志賀 富士弥 (外1名)

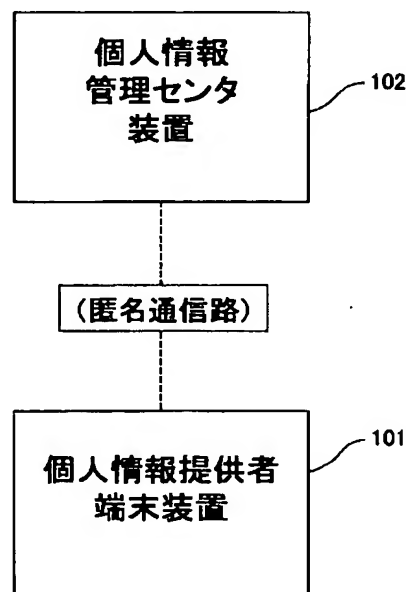
最終頁に続く

(54) 【発明の名称】 個人情報管理装置、個人情報管理方法、及び個人情報管理装置または方法を実行するプログラムを記録した記録媒体

(57) 【要約】

【課題】 管理センタを介してネットワークによる個人情報提供では、プライバシーを守るのが難しいし、第三者に漏れる恐れがある。

【解決手段】 個人情報を他者に提供しようとする個人情報提供者端末装置101に関する個人情報を、それぞれ単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割した上で個人情報管理センタ装置102に登録し、それらの間の関連は個人情報提供者の持つ端末でのみ保持することで、個人情報管理センタでは個人情報提供者のプライバシーを把握できなくする。また、個人情報利用者に対しては、個人情報管理センタに登録された部分個人情報の識別子と、個人情報取得許諾条件をセットにして提供し、取得許諾条件に合う場合にのみ個人情報を提供する。



## 【特許請求の範囲】

【請求項1】 個人情報提供者端末装置で提供する個人情報  
を通信手段を介して個人情報管理センタ装置に登録  
し、個人情報利用者端末装置が前記個人情報を通信手段  
を介して取得して利用する個人情報管理装置であって、  
前記個人情報提供者端末装置は、入力された個人情報を  
単独では特定の個人との関連づけができずに意味をなさ  
ない部分個人情報に分割するための個人情報分割手段  
と、この部分個人情報を前記個人情報管理センタ装置に  
送信する手段と、前記個人情報管理センタ装置で部分個  
10 個人情報に対して生成した部分個人情報識別子を受信する  
手段と、前記受信した部分個人情報識別子によって表さ  
れる部分個人情報の内容と対応づけて保存する部分個人  
情報関連記憶手段と、提供しようとする部分個人情報に  
対応した部分個人情報識別子を前記部分個人情報関連記  
憶手段から取得して前記個人情報利用者端末装置に送信  
する手段とを備えたことを特徴とする個人情報管理装  
置。

【請求項2】 請求項1の個人情報管理装置において、  
前記個人情報提供者端末装置は、前記部分個人情報識別  
子を部分個人情報関連記憶手段から取り出して前記個人  
情報管理センタ装置に送信する手段と、前記個人情報管  
理センタ装置から部分個人情報識別子に対応する部分個  
20 人情報を受信する手段と、前記受信した前記部分個人情  
報を出力する手段を備えたことを特徴とする個人情報管  
理装置。

【請求項3】 請求項1の個人情報管理装置において、  
前記個人情報提供者端末装置は、変更しようとする個人  
情報を入力する手段と、前記個人情報分割手段によって  
分割された部分個人情報の内容に応じた部分個人情報識  
30 別子を前記部分個人情報関連記憶手段から検索する手段  
と、前記部分個人情報とその識別子とを対にして前記個人  
情報管理センタ装置に送信する手段とを備えたことを特  
徴とする個人情報管理装置。

【請求項4】 請求項1の個人情報管理装置において、  
前記個人情報提供者端末装置は、前記部分個人情報関連  
記憶手段から提供したい部分個人情報に対応した部分個  
人情報識別子を取り出す手段と、前記個人情報利用者端  
末装置にどのような部分個人情報をどのような条件で提  
40 供するのかを表す部分個人情報利用許諾情報を生成する  
手段と、前記個人情報利用者端末装置に対して前記部分  
個人情報利用許諾情報を送信する手段とを備えたことを  
特徴とする個人情報管理装置。

【請求項5】 請求項3の個人情報管理装置において、  
前記個人情報提供者端末装置は、提供する個人情報を前  
記個人情報分割手段で分割した部分個人情報を暗号化す  
るための暗号鍵を生成する手段と、各部分個人情報を前  
記暗号鍵を用いて暗号化する手段と、前記暗号化部分個  
50 人情報をそれぞれ別個に前記個人情報管理センタ装置に  
送信する手段と、前記個人情報管理センタ装置で生成し

受信した部分個人情報識別子を、それによって表される  
部分個人情報の内容および、暗号化に用いた前記暗号化  
鍵と対応づけて前記部分個人情報関連記憶手段に保存す  
る手段とを備えことを特徴とする個人情報管理装置。

【請求項6】 個人情報提供者端末装置で提供する個人  
情報を通信手段を介して個人情報管理センタ装置に登録  
し、個人情報利用者端末装置が前記個人情報を通信手段  
を介して取得して利用する個人情報管理装置であって、  
前記個人情報管理センタ装置は、個人情報を単独では  
特定の個人との関連づけができずに意味をなさない部分  
10 個人情報に分割した部分個人情報を前記個人情報提供者  
端末装置から受信する手段と、前記受信した部分個人情  
報に識別子を生成する識別子生成手段と、該生成した部  
分個人情報識別子と前記部分個人情報とを対応させて保  
存する部分個人情報記憶手段と、前記部分個人情報識別  
子を個人情報提供者端末装置に送信する手段と、前記個  
人情報利用者端末装置から受信した部分個人情報識別子  
に対応する部分個人情報を前記部分個人情報記憶手段か  
ら検索する手段と、前記検索された部分個人情報を前記  
20 個人情報提供者端末装置に送信する手段とを備えたこと  
を特徴とする個人情報管理装置。

【請求項7】 請求項6の個人情報管理装置において、  
前記個人情報管理センタ装置は、前記個人情報提供者端  
末装置が変更しようとする前記部分個人情報と該部分個  
人情報の内容に応じた部分個人情報識別子を受信する手  
段と、前記受信した部分個人情報識別子を用いて前記部  
分個人情報を検索してその値を受信した部分個人情報の  
値に変更する手段とを備えたことを特徴とする個人情報  
管理装置。

【請求項8】 請求項6の個人情報管理装置において、  
前記個人情報管理センタ装置は、個人情報利用者端末装  
置が利用しようとする部分個人情報に対応した部分個人  
情報利用許諾情報を受信する手段と、前記受信した部分  
個人情報利用許諾情報が、当該個人情報利用者端末装置  
に対して、指定された部分個人情報の利用を許諾したも  
のかどうかを検証する利用条件判断手段と、前記検証が  
成功した場合に前記部分個人情報利用許諾情報に指定さ  
れた部分個人情報識別子に対応する部分個人情報を前記  
部分個人情報記憶手段から検索する手段と、前記検索し  
40 た部分個人情報を前記個人情報利用者端末装置に送信す  
る手段とを備えたことを特徴とする個人情報管理装置。

【請求項9】 請求項8の個人情報管理装置において、  
前記個人情報管理センタ装置は、前記受信した部分個人  
情報利用許諾情報が条件を満たしていることを確認した  
ときに該部分個人情報利用許諾情報に指定された部分個  
人情報識別子に対応する部分個人情報を前記部分個人情  
報記憶装置から検索する手段と、前記検索した部分個人  
情報の列の順序をランダムに入れ換える部分個人情報順  
序入換手段と、前記順序の入れ換えられた部分個人情報  
50 の列を前記個人情報利用者端末装置に送信する手段とを

備えたことを特徴とする個人情報管理装置。

【請求項 1 0】 請求項 7 の個人情報管理装置において、  
前記個人情報管理センタ装置は、前記個人情報提供者端末装置が部分個人情報を暗号鍵を用いて暗号化した部分個人情報を受信する手段と、前記受信した暗号化部分個人情報に対応した部分個人情報識別子を生成する部分個人情報識別子生成手段と、前記生成した部分個人情報識別子と前記提供者暗号化部分個人情報とを対応させて前記部分個人情報記憶手段に保存する手段と、前記部分個人情報識別子を前記個人情報提供者端末装置に送信する手段とを備えたことを特徴とする個人情報管理装置。

【請求項 1 1】 請求項 9 の個人情報管理装置において、  
前記個人情報管理センタ装置は、前記個人情報利用者端末装置が利用しようとする部分個人情報に対応した部分個人情報利用許諾情報を受信する手段と、前記受信した部分個人情報利用許諾情報が、当該個人情報利用者端末装置に対して、指定された部分個人情報の利用を許諾したものかどうかを検証する利用条件判断手段と、前記検証が成功した場合に前記部分個人情報利用許諾情報に指定された部分個人情報識別子に対応する部分個人情報を前記部分個人情報記憶手段から検索する手段と、前記検索した部分個人情報を前記個人情報利用者端末装置に送信する手段とを備えたことを特徴とする個人情報管理装置。

【請求項 1 2】 請求項 1 1 の個人情報管理装置において、  
前記個人情報管理センタ装置は、前記部分個人情報利用許諾情報に指定された部分個人情報識別子に対応する部分個人情報を前記部分個人情報記憶装置から検索する手段と、各提供者暗号化部分個人情報を個人情報管理センタ装置のみが知る鍵を用いて暗号化してセンタ暗号化提供者暗号化部分個人情報の列を得て前記個人情報利用者端末装置に送信する手段と、前記個人情報利用者端末装置から受信した前記利用者暗号化センタ暗号化部分個人情報の列に含まれる利用者暗号化センタ暗号化部分個人情報をそれぞれ鍵を用いて復号する手段と、前記復号した利用者暗号化部分個人情報の列の順序をランダムに入れ換える部分個人情報順序入換手段と、前記入れ換えた利用者暗号化部分個人情報の列を前記個人情報利用者端末装置に送信する手段とを備えたことを特徴とする個人情報管理装置。

【請求項 1 3】 個人情報提供者端末装置で提供する個人情報を通信手段を介して個人情報管理センタ装置に登録し、個人情報利用者端末装置が前記個人情報を通信手段を介して取得して利用する個人情報管理装置であって、  
前記個人情報利用者端末装置は、前記個人情報提供者端末装置から提供したい部分個人情報に対応した部分個人

情報識別子を受信する手段と、前記受信した個人情報識別子を部分個人情報識別子記憶装置に保存する手段と、前記保存した部分個人情報識別子を前記個人情報管理センタ装置に送信する手段と、前記送信に対して前記個人情報管理センタ装置から部分個人情報識別子に対応する部分個人情報を受信する手段と、該受信した部分個人情報を出力する手段とを備えたことを特徴とする個人情報管理装置。

【請求項 1 4】 請求項 1 3 の個人情報管理装置において、  
前記個人情報利用者端末装置は、前記個人情報提供者端末装置から提供したい部分個人情報についてどのような部分個人情報をどのような条件で提供するのかを表す部分個人情報利用許諾情報を受信する手段と、前記受信した部分個人情報利用許諾情報を部分個人情報利用許諾情報記憶手段に保存することを特徴とする個人情報管理装置。

【請求項 1 5】 請求項 1 3 の個人情報管理装置において、  
前記個人情報利用者端末装置は、利用したい部分個人情報に対応した部分個人情報利用許諾情報を前記部分個人情報利用許諾情報記憶手段から取り出す手段と、該取り出した前記部分個人情報利用許諾情報を前記個人情報管理センタ装置に送信する手段と、前記部分個人情報利用許諾情報に対して個人情報管理センタ装置報により指定された部分個人情報の利用を許諾したことを検証し、該部分個人情報利用許諾情報に指定された部分個人情報識別子に対応する部分個人情報を受信する手段と、前記受信した部分個人情報を出力する手段とを備えたことを特徴とする個人情報管理装置。

【請求項 1 6】 請求項 1 5 の個人情報管理装置において、  
前記個人情報利用者端末装置は、前記個人情報管理センタ装置から前記部分個人情報利用許諾情報に対して検索した部分個人情報の列の順序をランダムに入れ換えたものを受信する手段と、前記受信した部分個人情報の列を出力する手段とを備えたことを特徴とする個人情報管理装置。

【請求項 1 7】 請求項 1 6 の個人情報管理装置において、  
前記個人情報利用者端末装置は、利用しようとする部分個人情報に対応した部分個人情報利用許諾情報を取得する手段と、前記取得した部分個人情報利用許諾情報を前記個人情報管理センタ装置に送信する手段と、前記個人情報管理センタ装置が前記部分個人情報利用許諾情報に対して検証および該部分個人情報利用許諾情報に指定された個人情報を受信する手段と、前記受信した個人情報を復号する手段と、前記復号した部分個人情報を出力する手段とを備えたことを特徴とする個人情報管理装置。

【請求項 1 8】 請求項 1 7 の個人情報管理装置において

て、

前記個人情報利用者端末装置は、前記個人情報管理センタ装置が前記部分個人情報利用許諾情報に対して検証および該部分個人情報利用許諾情報に指定された個人情報を該個人情報管理センタ装置のみが知る鍵を用いて暗号化した提供者暗号化部分個人情報の列を受信する手段と、前記受信した提供者暗号化部分個人情報を復号する手段と、前記暗号化部分を個人情報利用者端末装置のみが知る鍵を用いて暗号化する手段と、前記暗号化した部分個人情報の列を前記個人情報管理センタ装置に送信する手段と、前記個人情報管理センタ装置が前記利用者暗号化センタ暗号化部分個人情報の列に含まれる利用者暗号化センタ暗号化部分個人情報を鍵を用いて復号し、部分個人情報の列の順序を入れ替えた利用者暗号化部分個人情報の列を受信する手段と、前記受信した利用者暗号化部分個人情報を復号する手段と、前記復号した部分個人情報を出力する手段とを備えたことを特徴とする個人情報管理装置。

【請求項 19】 個人情報提供者端末装置で提供する個人情報を通信手段を介して個人情報管理センタ装置に登録し、個人情報利用者端末装置が前記個人情報を通信手段を介して取得して利用する個人情報管理方法であって、

前記個人情報提供者端末装置は、入力された個人情報を単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割し、この部分個人情報を前記個人情報管理センタ装置に送信し、前記個人情報管理センタ装置で部分個人情報に対して生成した部分個人情報識別子を受信し、前記受信した部分個人情報識別子によって表される部分個人情報の内容と対応づけて保存し、提供しようとする部分個人情報に対応した部分個人情報識別子を前記個人情報関連記憶手段から取得して前記個人情報利用者端末装置に送信することを特徴とする個人情報管理方法。

【請求項 20】 個人情報提供者端末装置で提供する個人情報を通信手段を介して個人情報管理センタ装置に登録し、個人情報利用者端末装置が前記個人情報を通信手段を介して取得して利用する個人情報管理方法であって、

前記個人情報管理センタ装置は、個人情報を単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割した部分個人情報を前記個人情報提供者端末装置から受信し、前記受信した部分個人情報に識別子を生成し、該生成した部分個人情報識別子と前記部分個人情報とを対応させて保存し、前記部分個人情報識別子を個人情報提供者端末装置に送信し、前記個人情報利用者端末装置から受信した部分個人情報識別子に対応する部分個人情報を前記部分個人情報記憶手段から検索し、前記検索された部分個人情報を前記個人情報提供者端末装置に送信することを特徴とする個人情報管理方

法。

【請求項 21】 個人情報提供者端末装置で提供する個人情報を通信手段を介して個人情報管理センタ装置に登録し、個人情報利用者端末装置が前記個人情報を通信手段を介して取得して利用する個人情報管理方法であって、

前記個人情報利用者端末装置は、前記個人情報提供者端末装置から提供したい部分個人情報に対応した部分個人情報識別子を受信し、前記受信した個人情報識別子を部分個人情報識別子記憶装置に保存し、前記保存した部分個人情報識別子を前記個人情報管理センタ装置に送信し、前記送信に対して前記個人情報管理センタ装置から部分個人情報識別子に対応する部分個人情報を受信し、該受信した部分個人情報を出力することを特徴とする個人情報管理方法。

【請求項 22】 請求項 1～5、請求項 13～18、請求項 19 または 21 のいずれか 1 項に記載の装置または方法における処理をコンピュータに実行させるためのプログラムを、該コンピュータが読み取り可能な記録媒体に記録したことを特徴とする個人情報管理装置または方法を実行するプログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ネットワークを通じて利用者の嗜好などの個人情報を収集する際に、利用者が自分の個人情報の利用方法を制御可能にするための個人情報管理方法および個人情報管理装置に関するものである。

【0002】

【従来の技術】 近年、インターネットなどのネットワークの発展により、双方向の通信を利用した情報提供手段が利用できるようになり、利用者から提供される利用者個人の嗜好などの個人情報を収集し、個々人の嗜好に適した情報や広告を提供する情報提供サービスが盛んに利用されるようになってきた。

【0003】 例えば、利用者の嗜好に応じて利用者の興味のありそうな情報を電子メールを通じて利用者に届けたり、利用者が WWW (World Wide Web) のコンテンツを閲覧する際にユーザに適した広告を表示したりといったサービスが行なわれている。また、ネットワークを通じて商品の販売を行なう業者は、商品販売の際に商品の提供に必要な配送先などの個人情報を収集できれば効率よい商取引が可能となる。

【0004】

【発明が解決しようとする課題】 上記のように、ネットワークの利用者が個人情報を提供する機会が増えているが、こういった個人情報の提供の際に人の手で逐一個人情報の入力と提供を行なっているのは利便性が悪いので、個人情報を個人情報管理センタに集めておき、それを利用することが考えられるが、それでは利用者のプライバ

シを個人情報管理センタに把握されてしまう問題があった。

【0005】また、このような目的で収集される個人情報は、一旦利用者が情報提供者に渡ししまえば、利用者はその情報の利用方法についてそれ以上制御することができなくなっていた。すなわち、情報提供者が収集した個人情報を利用者が同意した方法以外に利用したり、第三者に提供される恐れがある。

【0006】このような課題を解決しようとする方式として、特開平9-91358号公報、特開平11-149504号公報、特開平11-273681号公報に開示された技術がある。

【0007】上記の特開平9-91358号公報の技術は、情報提供者と受信者との間で送受信要件を通信し、双方の希望が満足される配信リストを生成する。しかし、第三者に対して送受信情報の開示を制限するものではないため、個人情報が第三者に提供される恐れがある。

【0008】特開平11-149504号公報の技術は、指定された参照者にのみ個人情報取得を許すものであるが、登録者から発行された問い合わせコードと参照者側からの応答との一致を確認してから参照者に個人情報を伝達する。しかし、送受信情報を判読不可能にするものではないため、情報漏れの恐れがある。

【0009】特開平11-273681号公報に技術は、許可されない参照者が個人情報を読み出しても解読不可能にすることを目的とする。そのために個人情報を基本情報ファイルと属性情報ファイルに分割し、暗号化コードで互に関連付けるものである。しかし、分割情報（暗号化コード）の伝達経路や格納場所で情報が漏れる恐れがある。

【0010】本発明の目的は、個人情報を提供することを許諾した者以外の、例えば個人情報の提供を仲介する個人情報管理センタにも個人情報の提供者のプライバシーを把握されないようにした個人情報管理装置および個人情報管理方法を提供することにある。

【0011】本発明の他の目的は、個人情報をその利用者に提供する際に、個人情報の利用方法に関し、個人情報の提供者が柔軟に制御ができるようにすること、特に、個人を特定できる形で情報を渡さずに、個人情報の統計的使用のみを許可できるようにする個人情報管理装置および個人情報管理方法を提供することにある。

【0012】

【課題を解決するための手段】本発明では、個人情報を他者に提供しようとする個人情報提供者に関する個人情報を、それぞれ単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割した上で個人情報管理センタに登録し、それらの間の関連は個人情報提供者の持つ端末でのみ保持することで、個人情報管理センタでは個人情報提供者のプライバシーを把握できなくす

る。

【0013】また、個人情報提供者から個人情報提供者の個人情報を利用しようとする個人情報利用者に対しては、個人情報管理センタに登録された部分個人情報の識別子と、個人情報取得許諾条件をセットにして提供し、取得許諾条件に合う場合にのみ個人情報管理センタが部分個人情報を個人情報利用者に提供することで個人情報の利用方法をユーザが制御する。

【0014】さらに、個人情報管理センタが個人情報利用者からの複数の取得要求を一括して受け付け、これに対する回答となる部分個人情報の順序をランダムに入れ換えて送信することで統計的利用に限った取得許諾を可能にする。

【0015】以上のことから、本発明は、以下の個人情報管理方法、個人情報管理装置、及び個人情報管理装置または方法を実行するプログラムを記録する記録媒体を特徴とする。

【0016】（個人情報提供者端末装置）個人情報提供者端末装置で提供する個人情報を通信手段を介して個人情報管理センタ装置に登録し、個人情報利用者端末装置が前記個人情報を通信手段を介して取得して利用する個人情報管理装置であって、前記個人情報提供者端末装置は、入力された個人情報を単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割するための個人情報分割手段と、この部分個人情報を前記個人情報管理センタ装置に送信する手段と、前記個人情報管理センタ装置で部分個人情報に対して生成した部分個人情報識別子を受信する手段と、前記受信した部分個人情報識別子によって表される部分個人情報の内容と対応づけて保存する部分個人情報関連記憶手段と、提供しようとする部分個人情報に対応した部分個人情報識別子を前記部分個人情報関連記憶手段から取得して前記個人情報利用者端末装置に送信する手段とを備えたことを特徴とする個人情報管理装置。

【0017】また、前記個人情報提供者端末装置は、前記部分個人情報識別子を部分個人情報関連記憶手段から取り出して前記個人情報管理センタ装置に送信する手段と、前記個人情報管理センタ装置から部分個人情報識別子に対応する部分個人情報を受信する手段と、前記受信した前記部分個人情報を出力する手段を備えたことを特徴とする個人情報管理装置。

【0018】また、前記個人情報提供者端末装置は、変更しようとする個人情報を入力する手段と、前記個人情報分割手段によって分割された部分個人情報の内容に応じた部分個人情報識別子を前記部分個人情報関連記憶手段から検索する手段と、前記部分個人情報とその識別子を対にして前記個人情報管理センタ装置に送信する手段とを備えたことを特徴とする個人情報管理装置。

【0019】また、前記個人情報提供者端末装置は、前記部分個人情報関連記憶手段から提供したい部分個人情報



報に対応した部分個人情報識別子を取り出す手段と、前記個人情報利用者端末装置にどのような部分個人情報をどのような条件で提供するかを表す部分個人情報利用許諾情報を生成する手段と、前記個人情報利用者端末装置に対して前記部分個人情報利用許諾情報を送信する手段とを備えたことを特徴とする個人情報管理装置。

【0020】また、前記個人情報提供者端末装置は、提供する個人情報を前記個人情報分割手段で分割した部分個人情報を暗号化するための暗号鍵を生成する手段と、各部分個人情報を前記暗号鍵を用いて暗号化する手段と、前記暗号化部分個人情報をそれぞれ別個に前記個人情報管理センタ装置に送信する手段と、前記個人情報管理センタ装置で生成し受信した部分個人情報識別子を、それによって表される部分個人情報の内容および、暗号化に用いた前記暗号化鍵と対応づけて前記部分個人情報関連記憶手段に保存する手段とを備えことを特徴とする個人情報管理装置。

【0021】（個人情報管理センタ装置）個人情報提供者端末装置で提供する個人情報を通信手段を介して個人情報管理センタ装置に登録し、個人情報利用者端末装置が前記個人情報を通信手段を介して取得して利用する個人情報管理装置であって、前記個人情報管理センタ装置は、個人情報を単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割した部分個人情報を前記個人情報提供者端末装置から受信する手段と、前記受信した部分個人情報に識別子を生成する識別子生成手段と、該生成した部分個人情報識別子と前記部分個人情報を対応させて保存する部分個人情報記憶手段と、前記部分個人情報識別子を個人情報提供者端末装置に送信する手段と、前記個人情報利用者端末装置から受信した部分個人情報識別子に対応する部分個人情報を前記部分個人情報記憶手段から検索する手段と、前記検索された部分個人情報を前記個人情報提供者端末装置に送信する手段とを備えたことを特徴とする個人情報管理装置。

【0022】また、前記個人情報管理センタ装置は、前記個人情報提供者端末装置が変更しようとする前記部分個人情報と該部分個人情報の内容に応じた部分個人情報識別子を受信する手段と、前記受信した部分個人情報識別子を用いて前記部分個人情報を検索してその値を受信した部分個人情報の値に変更する手段とを備えたことを特徴とする個人情報管理装置。

【0023】また、前記個人情報管理センタ装置は、個人情報利用者端末装置が利用しようとする部分個人情報に対応した部分個人情報利用許諾情報を受信する手段と、前記受信した部分個人情報利用許諾情報が、当該個人情報利用者端末装置に対して、指定された部分個人情報の利用を許諾したものであるかどうかを検証する利用条件判断手段と、前記検証が成功した場合に前記部分個人情報利用許諾情報に指定された部分個人情報識別子に対応す

る部分個人情報を前記部分個人情報記憶手段から検索する手段と、前記検索した部分個人情報を前記個人情報利用者端末装置に送信する手段とを備えたことを特徴とする個人情報管理装置。

【0024】また、前記個人情報管理センタ装置は、前記受信した部分個人情報利用許諾情報が条件を満たしていることを確認したときに該部分個人情報利用許諾情報に指定された部分個人情報識別子に対応する部分個人情報を前記部分個人情報記憶装置から検索する手段と、前記検索した部分個人情報の列の順序をランダムに入れ換える部分個人情報順序入換手段と、前記順序の入れ換えられた部分個人情報の列を前記個人情報利用者端末装置に送信する手段とを備えたことを特徴とする個人情報管理装置。

【0025】また、前記個人情報管理センタ装置は、前記個人情報提供者端末装置が部分個人情報を暗号鍵を用いて暗号化した部分個人情報を受信する手段と、前記受信した暗号化部分個人情報に対応した部分個人情報識別子を生成する部分個人情報識別子生成手段と、前記生成した部分個人情報識別子と前記提供者暗号化部分個人情報とを対応させて前記部分個人情報記憶手段に保存する手段と、前記部分個人情報識別子を前記個人情報提供者端末装置に送信する手段とを備えたことを特徴とする個人情報管理装置。

【0026】また、前記個人情報管理センタ装置は、前記個人情報利用者端末装置が利用しようとする部分個人情報に対応した部分個人情報利用許諾情報を受信する手段と、前記受信した部分個人情報利用許諾情報が、当該個人情報利用者端末装置に対して、指定された部分個人情報の利用を許諾したものであるかどうかを検証する利用条件判断手段と、前記検証が成功した場合に前記部分個人情報利用許諾情報に指定された部分個人情報識別子に対応する部分個人情報を前記部分個人情報記憶手段から検索する手段と、前記検索した部分個人情報を前記個人情報利用者端末装置に送信する手段とを備えたことを特徴とする個人情報管理装置。

【0027】また、前記個人情報管理センタ装置は、前記部分個人情報利用許諾情報に指定された部分個人情報識別子に対応する部分個人情報を前記部分個人情報記憶装置から検索する手段と、各提供者暗号化部分個人情報を個人情報管理センタ装置のみが知る鍵を用いて暗号化してセンタ暗号化提供者暗号化部分個人情報の列を得て前記個人情報利用者端末装置に送信する手段と、前記個人情報利用者端末装置から受信した前記利用者暗号化センタ暗号化部分個人情報の列に含まれる利用者暗号化センタ暗号化部分個人情報をそれぞれ鍵を用いて復号する手段と、前記復号した利用者暗号化部分個人情報の列の順序をランダムに入れ換える部分個人情報順序入換手段と、前記入れ換えた利用者暗号化部分個人情報の列を前記個人情報利用者端末装置に送信する手段とを備えたこ

10

20

30

40

50

とを特徴とする個人情報管理装置。

【0028】（個人情報利用者端末装置）個人情報提供者端末装置で提供する個人情報を通信手段を介して個人情報管理センタ装置に登録し、個人情報利用者端末装置が前記個人情報を通信手段を介して取得して利用する個人情報管理装置であって、前記個人情報利用者端末装置は、前記個人情報提供者端末装置から提供したい部分個人情報に対応した部分個人情報識別子を受信する手段と、前記受信した個人情報識別子を部分個人情報識別子記憶装置に保存する手段と、前記保存した部分個人情報識別子を前記個人情報管理センタ装置に送信する手段と、前記送信に対して前記個人情報管理センタ装置から部分個人情報識別子に対応する部分個人情報を受信する手段と、該受信した部分個人情報を出力する手段とを備えたことを特徴とする個人情報管理装置。

【0029】また、前記個人情報利用者端末装置は、前記個人情報提供者端末装置から提供したい部分個人情報についてどのような部分個人情報をどのような条件で提供するのかを表す部分個人情報利用許諾情報を受信する手段と、前記受信した部分個人情報利用許諾情報を部分個人情報利用許諾情報記憶手段に保存することを特徴とする個人情報管理装置。

【0030】また、前記個人情報利用者端末装置は、利用したい部分個人情報に対応した部分個人情報利用許諾情報を前記部分個人情報利用許諾情報記憶手段から取り出す手段と、該取り出した前記部分個人情報利用許諾情報を前記個人情報管理センタ装置に送信する手段と、前記部分個人情報利用許諾情報に対して個人情報管理センタ装置報により指定された部分個人情報の利用を許諾したことを検証し、該部分個人情報利用許諾情報に指定された部分個人情報識別子に対応する部分個人情報を受信する手段と、前記受信した部分個人情報を出力する手段とを備えたことを特徴とする個人情報管理装置。

【0031】また、前記個人情報利用者端末装置は、前記個人情報管理センタ装置から前記部分個人情報利用許諾情報に対して検索した部分個人情報の列の順序をランダムに入れ換えたものを受信する手段と、前記受信した部分個人情報の列を出力する手段とを備えたことを特徴とする個人情報管理装置。

【0032】また、前記個人情報利用者端末装置は、利用しようとする部分個人情報に対応した部分個人情報利用許諾情報を取得する手段と、前記取得した部分個人情報利用許諾情報を前記個人情報管理センタ装置に送信する手段と、前記個人情報管理センタ装置が前記部分個人情報利用許諾情報に対して検証および該部分個人情報利用許諾情報に指定された個人情報を受信する手段と、前記受信した個人情報を復号する手段と、前記復号した部分個人情報を出力する手段とを備えたことを特徴とする個人情報管理装置。

【0033】また、前記個人情報利用者端末装置は、前

記個人情報管理センタ装置が前記部分個人情報利用許諾情報に対して検証および該部分個人情報利用許諾情報に指定された個人情報を該個人情報管理センタ装置のみが知る鍵を用いて暗号化した提供者暗号化部分個人情報の列を受信する手段と、前記受信した提供者暗号化部分個人情報を復号する手段と、前記暗号化部分を個人情報利用者端末装置のみが知る鍵を用いて暗号化する手段と、前記暗号化した部分個人情報の列を前記個人情報管理センタ装置に送信する手段と、前記個人情報管理センタ装置が前記利用者暗号化センタ暗号化部分個人情報の列に含まれる利用者暗号化センタ暗号化部分個人情報を鍵を用いて復号し、部分個人情報の列の順序を入れ替えた利用者暗号化部分個人情報の列を受信する手段と、前記受信した利用者暗号化部分個人情報を復号する手段と、前記復号した部分個人情報を出力する手段とを備えたことを特徴とする個人情報管理装置。

【0034】（個人情報管理方法）個人情報提供者端末装置で提供する個人情報を通信手段を介して個人情報管理センタ装置に登録し、個人情報利用者端末装置が前記個人情報を通信手段を介して取得して利用する個人情報管理方法であって、前記個人情報提供者端末装置は、入力された個人情報を単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割し、この部分個人情報を前記個人情報管理センタ装置に送信し、前記個人情報管理センタ装置で部分個人情報に対して生成した部分個人情報識別子を受信し、前記受信した部分個人情報識別子によって表される部分個人情報の内容と対応づけて保存し、提供しようとする部分個人情報に対応した部分個人情報識別子を前記個人情報関連記憶手段から取得して前記個人情報利用者端末装置に送信することを特徴とする個人情報管理方法。

【0035】個人情報提供者端末装置で提供する個人情報を通信手段を介して個人情報管理センタ装置に登録し、個人情報利用者端末装置が前記個人情報を通信手段を介して取得して利用する個人情報管理方法であって、前記個人情報管理センタ装置は、個人情報を単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割した部分個人情報を前記個人情報提供者端末装置から受信し、前記受信した部分個人情報に識別子を生成し、該生成した部分個人情報識別子と前記部分個人情報とを対応させて保存し、前記部分個人情報識別子を個人情報提供者端末装置に送信し、前記個人情報利用者端末装置から受信した部分個人情報識別子に対応する部分個人情報を前記部分個人情報記憶手段から検索し、前記検索された部分個人情報を前記個人情報提供者端末装置に送信することを特徴とする個人情報管理方法。

【0036】個人情報提供者端末装置で提供する個人情報を通信手段を介して個人情報管理センタ装置に登録し、個人情報利用者端末装置が前記個人情報を通信手段

10

20

30

40

50



を介して取得して利用する個人情報管理方法であって、前記個人情報利用者端末装置は、前記個人情報提供者端末装置から提供したい部分個人情報に対応した部分個人情報識別子を受信し、前記受信した個人情報識別子を部分個人情報識別子記憶装置に保存し、前記保存した部分個人情報識別子を前記個人情報管理センタ装置に送信し、前記送信に対して前記個人情報管理センタ装置から部分個人情報識別子に対応する部分個人情報を受信し、該受信した部分個人情報を出力することを特徴とする個人情報管理方法。

【0037】（記録媒体）前記の装置または方法における処理をコンピュータに実行させるためのプログラムを、該コンピュータが読み取り可能な記録媒体に記録したことを特徴とする個人情報管理装置または方法を実行するプログラムを記録した記録媒体。

【0038】

【発明の実施の形態】（実施形態1）個人情報の管理委託

本実施形態は、次のように実施することで、個人情報提供者のプライバシーを知られることなしに、個人情報提供者の個人情報の管理を個人情報管理センタに任せることにより、個人情報を保存しておくには十分な容量を持たない個人情報提供者端末装置を用いて、個人情報提供者の個人情報を参照することができるようにするものであり、以下に詳細に説明する。

【0039】（システム構成）図1は、本実施形態を示すシステム構成図である。システムは、個人情報を提供する側のユーザが利用する個人情報提供者端末装置101と、個人情報提供者端末装置101から受け取った個人情報を管理し、個人情報提供者端末装置101の必要に応じて個人情報を送信する個人情報管理センタ装置102とから構成される。各装置は互いにネットワークを通じて通信するものとする。

【0040】なお、個人情報提供者端末装置101と個人情報管理センタ装置102との間の通信は、個人情報管理センタ装置102から見て通信をしている個人情報提供者端末装置101を特定できないような匿名通信路を用いて行なってもよい。

【0041】（各装置の構成）図2に個人情報提供者端末装置101の構成を示す。個人情報提供者端末装置101は、個人情報管理センタ装置102と通信するための通信機能201と、個人情報を入力するための個人情報入力機能202と、個人情報を個々の部分に分割するための個人情報分割機能203と、部分に分けられて個人情報管理センタ装置102に送信した個人情報の関連と意味を保存する部分個人情報関連DB（データベース）204と、個人情報管理センタ装置102から送られた個人情報を出力する個人情報出力機能205とから構成される。

【0042】図3に個人情報管理センタ装置102の構

成を示す。個人情報管理センタ装置102は、個人情報提供者端末装置101と通信するための通信機能301と、部分個人情報識別子を生成する部分個人情報識別子生成機能302と、分割された個々の個人情報を保存する部分個人情報DB303とから構成される。

【0043】（処理の概要）本実施形態の処理は、個人情報提供者端末装置101が個人情報管理センタ装置102に対して個人情報を登録する個人情報登録処理と、個人情報提供者端末装置101が個人情報管理センタ装置102から登録済みの個人情報を取得する個人情報取得処理とから構成される。

【0044】（個人情報登録）図4に個人情報の登録処理の流れを示す。まずステップ401において、個人情報提供者端末装置101は個人情報を提供する者の個人情報を入力する。ここで個人情報とは、例えばその提供者の氏名、郵便番号、住所、年齢、性別などの他、趣味、好きな音楽のジャンル、髪の色、身長、体重など、上記提供者の特徴を表すどのような情報でもよい。ここでは一つの例として図17のような情報が入力されたものとする。

【0045】ステップ402において、個人情報分割機能703によって、入力された個人情報を、それぞれ単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割する。このような分割方法として、例えば、図18に示すように、上記の名前～趣味までの情報をそれぞれ別個の部分個人情報となるように分割してもよい。この場合、“Alice”，“111”などの部分個人情報を単独で与えても、Aliceという人物がどのような人物であるかを知ることができない。これらの部分個人情報は、“Alice”がその人物の名前であり、“111”がその人物の住所の郵便番号であり、“1-1 Southern Ave”がその人物の住所であり……といった事実、すなわち、これらの部分個人情報がその特定の人物によって結びつけられているという部分個人情報間の関連を知らなければ意味をなさない。

【0046】あるいは、図19に示すように、より細かく文字を単位に分割してもよい。この場合、“A”がその人物の名前の一文字目であり、“1”がその人物の名前の二文字目であり、……という部分個人情報間の関連を知ることがなければ“Alice”という単語すら知られることはない。

【0047】さらに、個人情報をビット列で表し、それを前から順に適切なビット数ずつ切り出したものを部分個人情報としてもよい。例えば、“Alice…”を01000,00101,10100,10110,00110,11001,01…とする。

【0048】ただし、これらの分割方法は、本発明の請求範囲を限定するものではなく、入力された個人情報をそれぞれ単独では特定の個人との関連づけができずに、意味をなさない部分個人情報に分割する方法であれば、

10

20

30

40

50

どのような方法を用いても構わない。

【0049】ステップ403において、個人情報提供者端末装置101は、上記部分個人情報をそれぞれ別個に個人情報管理センタ装置102に送信する。例えば“Alice”を送信したとする。

【0050】ステップ404において、個人情報管理センタ装置102は、部分個人情報識別子生成機能802によって受信した部分個人情報に対応した識別子（部分個人情報識別子）を生成する。ここで、個人情報管理センタ装置102がシステム内に複数存在する場合には、個人情報管理センタ装置102を特定する個人情報管理センタ識別子が上記部分個人情報識別子に含まれるようにしてもよい。

【0051】ステップ405において、生成した上記部分個人情報識別子と上記部分個人情報とを対応させて部分個人情報DB303に保存する。図10に部分個人情報DBの構成例を示す。ただし、図10は部分個人情報DBの構成を限定するものではなく、部分個人情報識別子と部分個人情報の対応関係を保持できるものであればどのような構成であってもよい。

【0052】ステップ406において、個人情報管理センタ装置102は上記部分個人情報識別子を個人情報提供者に送信する。

【0053】ステップ407において、個人情報提供者端末装置は上記部分個人情報識別子を、それによって表される部分個人情報の内容と対応づけて部分個人情報関連DB204に保存する。このとき、個人情報管理センタ装置102に送信した部分個人情報の値とも関連づけて保存してもよい。図11に部分個人情報関連DB204の構成例を示す。ただし、図11は部分個人情報関連DB204の構成を限定するものではなく、部分個人情報識別子と部分個人情報の内容の対応関係を保持できるものであればどのような構成であってもよい。

【0054】ステップ402で分割した全ての部分個人情報に対して、ステップ403からステップ406までの処理を繰り返す。個人情報管理センタ装置が複数ある場合には、それぞれの部分個人情報を異なる個人情報管理センタ装置に送信してもよい。

【0055】個人情報提供者端末装置101と個人情報管理センタ装置102の間の通信が匿名通信路を介して行なわれる場合には、個人情報管理センタ装置102は個々の部分個人情報が同一の個人情報提供者によるものであることが分からないため、個人情報管理センタ装置102は個人情報提供者のプライバシーを知ることがない。個人情報管理センタ装置102が、個々の部分個人情報が関連するものであることを推測できないようにするために、各部分個人情報に対するステップ403からステップ406までの処理を連続して行なわずに、適宜時間間隔において処理してもよい。

【0056】このようにして、例えば、部分個人情報関

連DB303には図20に示すような情報が保存される。ここで、id<sub>1</sub>~id<sub>6</sub>は部分個人情報識別子である。また、例えば部分個人情報関連DB204には図21に示すような情報が保存される。

【0057】（個人情報取得）図5に個人情報の取得処理の流れを示す。まず、ステップ501において、個人情報提供者端末装置101は、利用したい部分個人情報の内容に対応した部分個人情報識別子を部分個人情報関連DB204から取り出す。

10 【0058】ステップ502において個人情報利用者端末装置101から個人情報管理センタ装置102に対し、上記部分個人情報識別子を送信する。個人情報管理センタ装置が複数存在する場合には、上記部分個人情報識別子に含まれる個人情報管理センタ識別子を利用して個人情報管理センタ装置を特定する。

【0059】ステップ503において、個人情報管理センタ装置102は、受信した部分個人情報識別子に対応する部分個人情報を、部分個人情報DB303から検索する。

20 【0060】ステップ504において、個人情報管理センタ装置102から個人情報提供者端末装置101に対し、検索された上記部分個人情報を送信する。

【0061】ステップ505において、個人情報提供者端末装置101は受信した上記部分個人情報を出力する。

【0062】（実施形態1のまとめ）以上のような手順を用いて、個人情報提供者の個人情報を個人情報管理センタ装置において管理することで、個人情報管理センタ装置に保存されている情報を見てもそれぞれの部分個人情報同士の関連が分からないため、個人情報管理センタ装置からDBのデータが漏洩しても個人情報提供者のプライバシーが守られる。

【0063】また、個人情報提供者端末装置と個人情報管理センタ装置との間の通信が匿名通信路を介して行なわれれば、個人情報管理センタ装置も、部分個人情報同士の関連を知ることが不可能となり、個人情報提供者のプライバシーを守るのに好適となる。

【0064】（実施形態2）個人情報提供の基本形  
本実施形態は、個人情報提供者の個人情報を分割した部分個人情報を個別に個人情報管理センタ装置102に保存し、ユーザ端末装置においてそれら部分個人情報間の関連づけを保存するためのものであり、以下に詳細に説明する。

【0065】（システム構成）図6は、本発明の実施形態を示すシステム構成図である。システムは、個人情報を提供する側のユーザが利用する個人情報提供者端末装置601と、個人情報を利用する側である個人情報利用者端末装置602と、個人情報提供者端末装置601から受け取った個人情報を管理し、個人情報利用者端末装置602に個人情報を必要に応じて提供する個人情報管

理センタ装置 603 とから構成される。

【0066】各装置は互いにネットワークを通じて通信するものとする。システム内には個々の個人情報の提供者および個人情報の利用者に対応した、それぞれ複数の個人情報提供者端末装置、個人情報利用者端末装置があってもよい。あるいは、複数の個人情報管理センタ装置があってもよい。

【0067】具体的には、例えば、個人情報利用者端末装置 602 は、ネットワーク上でコンテンツを販売し、コンテンツの購入者の嗜好情報を集計して商品のマーケティングに利用したいと考えるコンテンツ販売業者によって利用される。一方、個人情報提供者端末装置 601 は、上記コンテンツ販売業者からコンテンツを購入するユーザによって利用されていてよい。ただし、この具体例は本発明の請求範囲を限定するものではない。

【0068】なお、個人情報提供者端末装置 601 と個人情報管理センタ装置 603 との間の通信は、個人情報管理センタ装置 603 から見て通信をしている個人情報提供者端末装置 601 を特定できないような匿名通信路を用いて行なってもよい。

【0069】（各装置の構成）図 7 に個人情報提供者端末装置 601 の構成を示す。個人情報提供者端末装置 601 は、個人情報管理センタ装置 603 および個人情報利用者端末装置 602 と通信するための通信機能 701 と、個人情報を入力するための個人情報入力機能 702 と、個人情報を個々の部分に分割するための個人情報分割機能 703 と、部分に分けられて個人情報管理センタ装置 603 に送信した個人情報の関連と意味を保存する部分個人情報関連 DB 704 とから構成される。

【0070】図 8 に個人情報管理センタ装置 603 の構成を示す。個人情報管理センタ装置 603 は、個人情報提供者端末装置 601 および個人情報利用者端末装置 602 と通信するための通信機能 801 と、部分個人情報識別子を生成する部分個人情報識別子生成機能 802 と、分割された個々の個人情報を保存する部分個人情報 DB 803 とから構成される。

【0071】図 9 に個人情報利用者端末装置 602 の構成を示す。個人情報利用者端末装置 602 は、個人情報提供者端末装置 601 および個人情報管理センタ装置 603 と通信するための通信機能 901 と、個人情報管理センタ装置から送られた個人情報を出力する個人情報出力機能 902 と、個人情報提供者端末装置 601 から送られた、個人情報管理センタ装置 603 に対して個人情報を問い合わせる際に利用する部分個人情報識別子を保存する部分個人情報識別子 DB 903 とから構成される。

【0072】（処理の概要）図 13 にシステム内で行なわれる処理の全体的な概要を示す。まず、ステップ 1301 で個人情報提供者端末装置 601 から個人情報提供者の個人情報を個人情報管理センタ装置 603 に送信

し、個人情報管理センタ装置 603 に上記個人情報を登録する。

【0073】次に、ステップ 1302 で個人情報提供者端末装置 601 から個人情報利用者端末装置 602 に対し、個人情報管理センタ装置 603 に登録された個人情報を識別するための情報を提供する。

【0074】最後に、ステップ 1303 で個人情報利用者端末装置 602 が個人情報管理センタ装置 603 から登録された個人情報を取得する。

10 【0075】（個人情報登録）図 14 に個人情報の登録処理の流れを示す。まず、ステップ 1401 において、個人情報提供者端末装置 601 は個人情報を提供する者の個人情報を入力する。ここで、個人情報とは、例えばその提供者の氏名、郵便番号、住所、年齢、性別などの他、趣味、好きな音楽のジャンル、髪の色、身長、体重など、上記提供者の特徴を表すどのような情報でもよい。ここでは一つの例として図 17 のような情報が入力されたものとする。

20 【0076】ステップ 1402 において、個人情報分割機能 703 によって、入力された個人情報を、それぞれ単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割する。このような分割方法として、例えば、図 18 に示すように、上記の名前～趣味までの情報をそれぞれ別個の部分個人情報となるように分割すること、あるいは、図 19 に示すように文字を単位に分割するなど、前記のステップ 402 による分割と同様のものでよい。

30 【0077】ステップ 1403 において、個人情報提供者端末装置 601 は、上記部分個人情報をそれぞれ別個に個人情報管理センタ装置 603 に送信する。例えば “A I i c e” を送信したとする。

【0078】ステップ 1404 において、個人情報管理センタ装置 603 は、部分個人情報識別子生成機能 802 によって受信した部分個人情報に対応した識別子（部分個人情報識別子）を生成する。ここで、個人情報管理センタ装置がシステム内に複数存在する場合には、個人情報管理センタ装置を特定する個人情報管理センタ識別子が上記部分個人情報識別子に含まれるようにしてもよい。

40 【0079】ステップ 1405 において、生成した上記部分個人情報識別子と上記部分個人情報とを対応させて部分個人情報 DB 803 に保存する。図 10 に部分個人情報 DB の構成例を示す。ただし、図 10 は部分個人情報 DB の構成を限定するものではなく、部分個人情報識別子と部分個人情報の対応関係を保持できるものであればどのような構成であってもよい。

【0080】ステップ 1406 において、個人情報管理センタ装置 603 は上記部分個人情報識別子を個人情報提供者に送信する。

50 【0081】ステップ 1407 において、個人情報提供

者は上記部分個人情報識別子を、それによって表される部分個人情報の内容と対応づけて部分個人情報関連DBに保存する。このとき、個人情報管理センタ装置603に送信した部分個人情報の値とも関連づけて保存してもよい。図11に部分個人情報関連DBの構成例を示す。ただし、図11は部分個人情報DBの構成を限定するものではなく、部分個人情報識別子と部分個人情報の内容の対応関係を保持できるものであればどのような構成であってもよい。

【0082】ステップ1402で分割した全ての部分個人情報に対して、ステップ1403からステップ1406までの処理を繰り返す。

【0083】個人情報管理センタ装置が複数ある場合には、それぞれの部分個人情報を異なる個人情報管理センタ装置に送信してもよい。また、個人情報提供者端末装置と個人情報管理センタ装置の間の通信が匿名通信路を介して行なわれる場合には、個人情報管理センタ装置は個々の部分個人情報、が同一の個人情報提供者によるものであることが分からないため、個人情報管理センタ装置は個人情報提供者のプライバシーを知ることがない。また、個人情報管理センタ装置が、個々の部分個人情報が関連するものであることを推測できないようにするために、各部分個人情報に対するステップ1403からステップ1406までの処理を連続して行なわずに、適宜時間間隔をおいて処理してもよい。

【0084】このようにして、例えば、部分個人情報DB803には図20に示すような情報が保存される。ここで、id<sub>1</sub>~id<sub>6</sub>は部分個人情報識別子である。

【0085】また、例えば部分個人情報関連DB704には図21に示すような情報が保存される。

【0086】（個人情報提供）図15に個人情報の提供処理の流れを示す。このような個人情報の提供処理は、具体的には例えば、コンテンツ販売業者がコンテンツを販売する際に、コンテンツの購入者から購入者の嗜好を取得したいような場合に、コンテンツ販売業者の利用する個人情報利用者端末から、上記購入者の利用する個人情報提供者端末に対して個人情報の提供を要求した場合などに行なわれる。ただし、この具体例は本発明の請求範囲を限定するものではない。

【0087】まず、ステップ1501において、個人情報提供者端末装置601は、部分個人情報関連DB704から提供したい部分個人情報に対応した部分個人情報識別子を取り出す。

【0088】ステップ1502において、個人情報提供者端末装置601から個人情報利用者端末装置602に対し、上記個人情報識別子を送信する。

【0089】ステップ1503において、個人情報利用者端末装置602は、受信した個人情報識別子を、部分個人情報識別子DB903に保存する。このとき、上記個人情報識別子を、上記個人情報提供者端末装置601

を利用する個人情報提供者と関連づけて保存してもよい。

【0090】ステップ1502において、個人情報提供者が提供しようとする複数の部分個人情報に対応する部分個人情報識別子を同時に送信し、ステップ1503において上記部分個人情報識別子を互いに関連づけて保存してもよい。あるいは個人情報提供者が提供しようとする複数の部分個人情報毎にステップ1502からステップ1503を繰り返してもよい。

【0091】図12に部分個人情報識別子DBの構成例を示す。ただし、図12は部分個人情報識別子DBの構成を限定するものではなく、部分個人情報識別子と個人情報提供者との関連を、個人情報の利用者の必要に応じて適宜保持するものであればどのような構成であってもよい。

【0092】（個人情報取得）図16に個人情報の取得処理の流れを示す。まず、ステップ1601において、個人情報利用者端末装置602は、利用したい部分個人情報に対応した部分個人情報識別子を部分個人情報識別子DB903から取り出す。

【0093】ステップ1602において個人情報利用者端末装置602から個人情報管理センタ装置に対し、上記部分個人情報識別子を送信する。個人情報管理センタ装置が複数存在する場合には、上記部分個人情報識別子に含まれる個人情報管理センタ識別子を利用して個人情報管理センタ装置を特定する。

【0094】ステップ1603において、個人情報管理センタ装置603は、受信した部分個人情報識別子に対応する部分個人情報を、部分個人情報DB803から検索する。

【0095】ステップ1604において、個人情報管理センタ装置603から個人情報利用者端末装置602に対し、検索された上記部分個人情報を送信する。

【0096】ステップ1605において、個人情報利用者端末装置602は受信した上記部分個人情報を出力する。

【0097】（実施形態2のまとめ）以上のような手順を用いて、個人情報提供者から個人情報利用者に対して個人情報を提供することで、個人情報管理センタ装置に保存されている情報を見てもそれぞれの部分個人情報同士の関連が分からないため、個人情報管理センタ装置からDBのデータが漏洩しても個人情報提供者のプライバシーが守られる。

【0098】また、個人情報提供者端末装置と個人情報管理センタ装置との間の通信が匿名通信路を介して行なわれれば、個人情報管理センタ装置も、部分個人情報同士の関連を知ることが不可能となり、個人情報提供者のプライバシーが守られる。

【0099】（実施形態3）個人情報の変更

本実施形態は、実施形態2で示したシステムにおいて、

個人情報提供者が一旦個人情報管理センタ装置に登録した個人情報を変更するためのものであり、以下に詳細に説明する。

【0100】（個人情報の変更）図22に個人情報の変更処理の流れを示す。まず、ステップ2201において、個人情報提供者端末装置は、変更しようとする個人情報を入力する。

【0101】ステップ2202において、個人情報分割機能によって、入力された個人情報を、それぞれ単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割する。この分割は、実施形態2におけるステップ1402と同様のものである。

【0102】ステップ2203において、分割されたそれぞれの上記部分個人情報の内容に応じた部分個人情報識別子を、部分個人情報関連DB704から検索する。

【0103】ステップ2204において、個人情報提供者端末装置601から個人情報管理センタ装置603に対し、入力され分割された上記部分個人と、検索された上記部分個人情報識別子とを対にして送信する。

【0104】ステップ2205において、個人情報管理センタ装置603は、部分個人情報DB803から受信した部分個人情報識別子を用いて検索し、対応する部分個人情報の値を受信した部分個人情報の値と置き換える。

【0105】ここで、ステップ2201からステップ2204において個人情報を新たに入力して送信する代わりに、部分個人情報識別子を、部分個人情報を消去するような指示とともに個人情報管理センタ装置603に送信することで、個人情報管理センタ装置603に登録された部分個人情報を消去し、以降個人情報利用者端末装置602からの個人情報取得要求に応えないようにすることもできる。

【0106】また、部分個人情報を変更する個人情報提供者端末装置が、確かに指定された部分個人情報識別子に対応する部分個人情報を登録した個人情報提供者端末装置であるかどうかを認証を行なってもよい。例えば、個人情報の登録処理において、個々の部分個人情報毎に匿名公開鍵を生成し、個人情報の変更処理時に、対応する秘密鍵を用いることで認証を行なってもよい。その場合には、例えば、部分個人情報DB803の1エントリ毎に匿名公開鍵の項を追加し、部分個人情報関連DB704の1エントリ毎に匿名公開鍵および秘密鍵の対の項を追加する。

【0107】図23、図24にそれぞれこの例の場合の部分個人情報DB803および部分個人情報関連DB704の構成例を示す。ただし、図23および図24は部分個人情報DBおよび部分個人情報関連DBの構成を限定するものではない。

【0108】この認証は、部分個人情報を変更する個人情報提供者端末装置が、確かに指定された部分個人情報

識別子に対応する部分個人情報を登録した個人情報提供者端末装置であることを確かめられる認証方式であればどのような方式を用いてもよい。また、個人情報管理センタ装置が、複数の部分個人情報が同一の個人情報提供者端末装置から登録されたものであることを知ることができないように、個別の部分個人情報に対して個別の認証を行なうようにしてもよい。例えば、部分個人情報識別子の発行毎にパスワードを設定し、そのパスワードを用いて認証してもよい。

10 【0109】（実施形態3のまとめ）以上のような手順を用いて、個人情報管理センタ装置に登録された個人情報を変更、あるいは消去することで、個人情報利用者端末装置が個人情報取得要求によって取得する個人情報を、個人情報提供者が必要に応じて制御することが可能となる。

【0110】具体的には、例えば、実施形態2で示した具体例において、Aliceが転居して住所が変更になった場合に、ステップ2204において（c、“2-2 Northern Ave.”）を送信することで、それ以降個人情報利用者端末装置が取得する個人情報の、住所の情報を変更することができる。

【0111】（実施形態4）部分個人情報利用許諾情報本実施形態は、個人情報提供者から個人情報利用者に対して部分個人情報識別子を提供する際に、その部分個人情報の利用に関する制限条件を課すものである。

【0112】本実施形態においては、実施形態2における個人情報管理センタ装置603を、図25のように構成する。ここで、個人情報管理センタ装置603は、個人情報提供者端末装置601および個人情報利用者端末装置602と通信するための通信機能2501と、部分個人情報識別子を生成する部分個人情報識別子生成機能2502と、分割された個々の個人情報を保存する部分個人情報DB2504と、部分個人情報に関する利用条件を判断する利用条件判断機能2503から構成される。

【0113】一方、個人情報利用者端末装置602は、図9における部分個人情報識別子DB903の代わりに部分個人情報利用許諾情報DBを持つ。

【0114】（個人情報提供）実施形態2において図15に示した個人情報提供処理の代わりに、図26に示す処理を行なう。

【0115】図26のステップ2601においては、個人情報提供者端末装置601は、部分個人情報関連DB704から提供したい部分個人情報に対応した部分個人情報識別子を取り出す。

【0116】ステップ2602において、個人情報利用者端末装置602にどのような部分個人情報をどのような条件で提供するのかを表す部分個人情報利用許諾情報を生成する。このような部分個人情報利用許諾情報としては、例えば図28のような構成の情報をを用いても良



い。

【0117】この部分個人情報利用許諾情報は、図28の個人情報利用者識別子2801で示される個人情報利用者は、部分個人情報識別子2803で示される部分個人情報を、個人情報利用条件2802で示される利用条件下であれば、部分個人情報管理センタから取得して利用することができることを表す。

【0118】ここで、部分個人情報識別子2803は、単一の部分個人情報識別子であってもよいし、複数の部分個人情報識別子の列であってもよい。後者の場合には、上記部分個人情報識別子の列に含まれる各部分個人情報識別子に対応する部分個人情報全体に対して個人情報利用条件が適用されることを表す。

【0119】ステップ2603において、個人情報提供者端末装置601から個人情報利用者端末装置602に対し、上記部分個人情報利用許諾情報を送信する。

【0120】ステップ2604において、個人情報利用者端末装置602は、受信した上記部分個人情報利用許諾情報を部分個人情報利用許諾情報DBに保存する。

【0121】（個人情報取得）実施形態2において図16に示した個人情報取得処理の代わりに、図27に示した処理を行なう。

【0122】まず、ステップ2701において、個人情報利用者端末装置602は、利用したい部分個人情報に対応した部分個人情報利用許諾情報を部分個人情報利用許諾情報DBから取り出す。

【0123】ステップ2702において、個人情報利用者端末装置602から個人情報管理センタ装置603に対し、上記部分個人情報利用許諾情報を送信する。

【0124】ステップ2703において、個人情報管理センタ装置603は、利用条件判断機能によって、受信した上記部分個人情報利用許諾情報が、確かに通信している個人情報利用者端末装置602に対して、指定された部分個人情報の利用を許諾したものであるかどうかを検証する。

【0125】上記検証が成功した場合、ステップ2704において、個人情報管理センタ装置603は、上記部分個人情報利用許諾情報に指定された部分個人情報識別子に対応する部分個人情報を、部分個人情報DB803から検索する。

【0126】ステップ2705において、個人情報管理センタ装置603から個人情報利用者端末装置601に対し、検索された上記部分個人情報を送信する。

【0127】ステップ2706において、個人情報利用者端末装置602は受信した上記部分個人情報を出力する。

【0128】上記ステップ2703における検証は、部分個人情報利用許諾情報の構成に応じて、その利用許諾を確かに検証できる方法であればどのようなものであってもよい。例えば、上記部分個人情報利用許諾情報が図

28のように構成されている場合には、まず通信をしている個人情報利用者端末装置が、個人情報利用者識別子2801によって示されるものであるかどうかを検証する。さらに、個人情報利用条件2802が満たされているかどうかを検証する。

【0129】（個人情報利用条件の定義）図28の個人情報利用条件2802としては、例えば、部分個人情報を取得することのできる期限を定めてもよい。また、部分個人情報の利用目的を限定してもよい。さらに、一定数以上の部分個人情報の取得を同時に行なわなければならないとしてもよい。さらにまた、部分個人情報に対して何らかの演算を加えた上で、個人情報管理センタ装置から個人情報利用者端末装置へ部分個人情報を送信することを条件とするなどの部分個人情報の提供の形態に関する条件を定めてもよい。もしくは、個人情報管理センタ装置から個人情報利用者端末装置に部分個人情報を送信する際に、一旦他の何らかの装置を経由してから送信するなどの部分個人情報の提供の方式に関する条件を定めてもよい。

【0130】ただし、これらの例は個人情報利用条件の内容を限定するものではなく、個人情報の提供および利用に関する条件であって、個人情報管理センタが検証可能なものであればどのような条件であってもよい。

【0131】（部分個人情報利用許諾情報の間接的提供）個人情報提供者端末装置601は、ステップ2603において、個人情報利用者識別子2801で示された個人情報利用者端末に直接部分個人情報利用許諾情報を送信しなくてもよい。

【0132】具体的には、例えば、コンテンツの配送を行なう業者の個人情報利用者識別子とコンテンツの配送先を表す部分個人情報に対応した部分個人情報識別子を指定した部分個人情報利用許諾情報を、コンテンツ購入要求とともにコンテンツの販売を行なう業者に対して送信し、上記販売業者が上記配送業者に対し、要求されたコンテンツとともに上記部分個人情報利用許諾情報を送信することで、上記配送業者のみがコンテンツの配送に必要な個人情報を取得できるようにしてもよい。ただし、この具体例は上記のような部分個人情報利用許諾情報の間接的提供の実施形態を限定するものではない。

【0133】（部分個人情報利用許諾情報への署名）部分個人情報利用許諾情報を、確かに個人情報提供者端末装置がステップ2602において生成したものであり、個人情報利用者端末装置あるいはその他の者が偽造したものではないことを、個人情報管理センタがステップ2703において検証してもよい。

【0134】例えば、個人情報の登録処理において、個々の部分個人情報毎に匿名公開鍵を生成し、対応する秘密鍵で、部分個人情報利用許諾情報に部分個人情報提供者端末装置の電子署名を加えてもよい。その場合、部分個人情報DB2504の1エントリごとに匿名公開鍵の

項を追加し、部分個人情報関連DB704の1エントリ毎に匿名公開鍵／秘密鍵のペアの項を追加する。ステップ2703における個人情報利用条件の判断の際には、部分個人情報識別子から対応する匿名公開鍵を調べ、これを用いて署名を検証することで、それが正しく上記個人情報提供者端末装置によって生成されたものであることを検証してもよい。あるいはこれ以外の方法を用いて上記検証を行なっても良い。

#### 【0135】（実施形態5）統計の利用

本実施形態は、個人情報利用条件として、「 $n$ 個以上の部分個人情報全体としての統計の利用であること」という条件を用いた場合である。

【0136】本実施形態においては、実施形態4における個人情報管理センタ装置603を、図29のように構成する。ここで、個人情報管理センタ装置603は、個人情報提供者端末装置601および個人情報利用者端末装置602と通信するための通信機能2901と、部分個人情報識別子を生成する部分個人情報識別子生成機能2902と、分割された個々の個人情報を保存する部分個人情報DB2905と、部分個人情報に関する利用条件を判断する利用条件判断機能2503とに加え、部分個人情報の列を個人情報利用者端末装置に送信する前に順序を入れ換える部分個人情報順序入換機能2904とから構成される。

【0137】（個人情報取得）図30に、個人情報取得処理の流れを示す。まず、ステップ3001において、個人情報利用者端末装置602は、利用したい部分個人情報に対応した部分個人情報利用許諾情報を部分個人情報識別子DB903から取り出す。このとき、個人情報利用条件を満たすため、必要な数 $n$ 個以上の部分個人情報利用許諾情報を取りだし、部分個人情報利用許諾情報の列とする。

【0138】ステップ3002において、個人情報利用者端末装置602から個人情報管理センタ装置603に対し、上記部分個人情報利用許諾情報の列を送信する。

【0139】ステップ3003において、個人情報管理センタ装置603は、利用条件判断機能によって、受信した上記部分個人情報利用許諾情報が、確かに通信している個人情報利用者端末装置に対して、指定された部分個人情報の利用を許諾したものであるかどうかを検証する。この中では同時に取得すべき部分個人情報の数 $n$ についても検証が行なわれる。このとき、部分個人情報利用許諾情報の列に含まれるすべての部分個人情報利用許諾情報が条件を満たしていることを確認する。

【0140】上記検証が成功した場合、ステップ3004において、個人情報管理センタ装置603は、上記部分個人情報利用許諾情報に指定された部分個人情報識別子に対応する部分個人情報を、部分個人情報DB803から検索し、部分個人情報の列とする。

【0141】ステップ3005において、部分個人情報

順序入換機能2904を用いて、上記部分個人情報の列の順序をランダムに入れ換える。

【0142】ステップ3006において、個人情報管理センタ装置603から個人情報利用者端末装置602に対し、順序の入れ換えられた上記部分個人情報の列を送信する。

【0143】ステップ3007において、個人情報利用者端末装置602は受信した上記部分個人情報の列を出力する。

【0144】個人情報利用者端末装置602は、順序を入れ換えられた部分個人情報を取得するため、個々の部分個人情報利用許諾情報が、どの部分個人情報に対応しているのかを知ることはなく、特定の個人に関する情報を入手することはできない。一方で、複数の部分個人情報全体として、例えば部分個人情報の値の平均値や、分布を求めるなどの統計処理に利用することが可能である。

【0145】具体的には、コンテンツの販売業者が、本実施形態での個人情報利用者端末装置を利用することで、コンテンツ購入者の個々の嗜好情報を入手することなしに、コンテンツ購入者の嗜好の傾向を統計的に入手することができる。ただし、この具体例は、本発明の適用範囲を限定するものではない。

【0146】（実施形態6）部分個人情報の暗号化  
本実施形態は、個人情報管理センタ装置603に登録する部分個人情報を、個人情報提供者端末装置601で暗号化してから個人情報管理センタ装置に送信するものである。

【0147】本実施形態においては、個人情報提供者端末装置601は、実施形態2における図7の構成に加え、部分個人情報を暗号化するための暗号化機能を持つ。

【0148】また、個人情報利用者端末装置602は、実施形態2における図9あるいは実施形態4における個人情報利用者端末装置の構成に加え、暗号化された部分個人情報を復号するための復号機能を持つ。

【0149】（個人情報登録）図31に、個人情報登録処理の流れを示す。まず、ステップ3101において、個人情報提供者端末装置602は個人情報を提供する者の個人情報を入力する。ここで個人情報とは、例えばその提供者の氏名、郵便番号、住所、年齢、性別などの他、趣味、好きな音楽のジャンル、髪の色、身長、体重など、上記提供者の特徴を表すどのような情報でもよい。ここでは一つの例として図17のような情報が入力されたものとする。

【0150】ステップ3102において、個人情報分割機能703によって、入力された個人情報を、それぞれ単独では特定の個人との関連づけができずに意味をなさない部分個人情報に分割する。このような分割方法として、例えば、図18に示すように、上記の名前～趣味ま

での情報をそれぞれ別個の部分個人情報となるように分割してもよい。あるいは、図19に示すように文字を単位に分割してもよい。

【0151】ステップ3103において、個人情報提供者端末装置601は、部分個人情報を暗号化するための暗号鍵を生成する。登録する部分個人情報全体で共通の暗号鍵を利用してもよいが、それぞれの部分個人情報ごとにことなる暗号鍵を生成してもよい。

【0152】ステップ3104において、それぞれの部分個人情報を暗号鍵を用いて暗号化する。例えば図33のような提供者暗号化部分個人情報を得る。ここで、 $E_{k1} \sim E_{k6}$ は、それぞれ暗号鍵 $k_1 \sim k_6$ による暗号化関数を表す。

【0153】ステップ3105において、個人情報提供者端末装置601は、上記提供者暗号化部分個人情報をそれぞれ別個に個人情報管理センタ装置603に送信する。例えば“ $E_{k1}(Alice)$ ”を送信したとする。

【0154】ステップ3106において、個人情報管理センタ装置603は、部分個人情報識別子生成機能802によって受信した暗号化部分個人情報に対応した識別子（部分個人情報識別子）を生成する。

【0155】ステップ3107において、生成した上記部分個人情報識別子と上記提供者暗号化部分個人情報とを対応させて部分個人情報DB803に保存する。部分個人情報DBは実施形態2の部分個人情報DBと同様の構成であってよい。

【0156】ステップ3108において、個人情報管理センタ装置603は上記部分個人情報識別子を個人情報提供者に送信する。

【0157】ステップ3109において、個人情報提供者は上記部分個人情報識別子を、それによって表される部分個人情報の内容および、暗号化に用いた暗号化鍵と対応づけて部分個人情報関連DB704に保存する。このとき、個人情報管理センタに送信した部分個人情報の値とも関連づけて保存してもよい。

【0158】ステップ3102で分割した全ての部分個人情報に対して、ステップ3105からステップ1406までの処理を繰り返す。

【0159】したがって、部分個人情報を暗号化して送信するため、個人情報提供者端末装置601と個人情報管理センタ装置603の間の通信が、匿名通信路を介して行なわれなくても、個人情報提供者のプライバシーが知られずに済む。

【0160】（個人情報提供）個人情報提供の際には、部分個人情報利用許諾情報に加え、その部分個人情報の暗号化に用いた暗号鍵を、個人情報提供者端末装置601から個人情報利用者端末装置602に送信する。個人情報利用者端末装置602は、受信した部分個人情報利用許諾情報と上記暗号鍵とを関連づけて部分個人情報利用許諾情報DBに保存する。

【0161】（個人情報取得）図32に個人情報取得処理の流れを示す。この処理では、図27に示す実施形態4の個人情報取得処理において、部分個人情報の代わりに提供者暗号化部分個人情報を、個人情報管理センタ装置から個人情報利用者端末装置に送信し、さらに、個人情報利用者端末装置が、上記提供者暗号化部分個人情報を復号するステップ3206が加わっている。

【0162】（実施形態7）暗号化と順序入換えの個人情報取得

10 本実施形態は、実施形態6の部分個人情報の暗号化を行なった上で、実施形態5と同様の部分個人情報の順序入換えを行なうものである。

【0163】本実施形態においては、個人情報管理センタ装置603は、実施形態5の図29の構成に加え、部分個人情報の暗号化／復号機能を持つ。また、個人情報利用者端末装置602は実施形態6の個人情報利用者端末装置の構成に加え、部分個人情報の暗号化機能を持つ。

【0164】また、個人情報提供者端末装置601および個人情報管理センタ装置603および個人情報利用者端末装置602が備える暗号化機能は、暗号化とは異なる順序で復号しても復号が可能な、順序の可換な暗号化を行なうものとする。

【0165】図34に、個人情報取得処理の流れを示す。ステップ3401からステップ3404までは、部分個人情報が暗号化されて提供者暗号化部分個人情報となっている以外は、図30のステップ3001からステップ3004までと同様である。

【0166】ステップ3405において、個人情報管理センタ装置603は、各提供者暗号化部分個人情報を個人情報管理センタ装置のみが知る鍵を用いて暗号化してセンタ暗号化提供者暗号化部分個人情報の列を得る。

【0167】ステップ3406において、個人情報管理センタ装置603から個人情報利用者端末装置602に対して上記センタ暗号化提供者暗号化部分個人情報の列を送信する。

【0168】ステップ3407において、個人情報利用者端末装置602は、上記センタ暗号化提供者暗号化部分個人情報の列に含まれるセンタ暗号化提供者暗号化部分個人情報をそれぞれ部分個人情報利用許諾情報に関連づけられた暗号鍵で復号し、センタ暗号化部分個人情報の列を得る。

【0169】ステップ3408において、個人情報利用者端末装置602は、上記センタ暗号化部分個人情報の列に含まれるセンタ暗号化部分個人情報を個人情報利用者端末装置のみが知る鍵を用いて暗号化して、利用者暗号化センタ暗号化部分個人情報の列を得る。

【0170】ステップ3409において、個人情報利用者端末装置602から個人情報管理センタ装置603に対して上記利用者暗号化センタ暗号化部分個人情報の列

を送信する。

【0171】ステップ3410において、個人情報管理センタ装置603は、上記利用者暗号化センタ暗号化部分個人情報の列に含まれる利用者暗号化センタ暗号化部分個人情報をそれぞれ上記個人情報管理センタ装置のみが知る鍵を用いて復号して利用者暗号化部分個人情報の列を得る。

【0172】ステップ3411において、部分個人情報順序入換機能を用いて、上記利用者暗号化部分個人情報の列の順序をランダムに入れ換える。

【0173】ステップ3412において、個人情報管理センタ装置603から個人情報利用者端末装置602に対し、順序の入れ換えられた上記利用者暗号化部分個人情報の列を送信する。

【0174】ステップ3413において、個人情報利用者端末装置602は受信した上記利用者暗号化部分個人情報の列を上記個人情報利用者端末装置のみが知る鍵を用いて復号し、部分個人情報の列を得る。

【0175】ステップ3414において、個人情報利用者端末装置602は上記部分個人情報の列を出力する。

【0176】上記個人情報管理センタ装置603のみが知る鍵は、常に同じ鍵を用いても、毎回異なる鍵を用いても良い。上記個人情報利用者端末装置のみが知る鍵は、同時に取得する部分個人情報の列全体に対して同一の鍵を用いていれば、常に同じ鍵を用いても、毎回異なる鍵を用いても良い。

【0177】なお、本発明の個人情報管理装置または方法における図4等の手順図で示した各実施形態例での処理の手順ないし計算アルゴリズムをコンピュータ等に実行させるためのプログラムを該コンピュータが読み取り可能な記録媒体、例えばフロッピー（登録商標）ディスクやメモ리카ード、MO、CD、DVDなどに記録して配布することが可能である。

【0178】

【発明の効果】以上のとおり、本発明によれば、以下の効果がある。

【0179】（1）（個人情報の分割）本発明は、個人情報提供者の個人情報を登録する個人情報管理センタ装置の持つデータベースの内容が万が一外部に漏洩することがあっても、個人情報提供者のプライバシーが知られることがない。

【0180】（2）（匿名で登録）本発明は、個人情報提供者の個人情報を登録する個人情報管理センタ装置においても、個人情報提供者のプライバシーが知られることがない。

【0181】（3）（識別子を渡す）本発明は、個人情報提供者のプライバシーを守った状態で、必要な個人情報に限り、個人情報利用者に対して個人情報を提供することができ、また、個人情報利用者が取得する個人情報の内容を、個人情報提供者が後から変更することができ

る。

【0182】（4）（個人情報取得許諾条件の利用）本発明は、不当な個人情報利用者が、あるいは不当な方法で個人情報提供者の個人情報を利用することを制限し、個人情報の利用を個人情報提供者が制御することができる。

【0183】（5）（統計的利用のみ）本発明は、個人情報利用者が、統計的な利用方法でのみ個人情報を利用し、特定の個人情報提供者の個人情報が把握されることがない。

【0184】（6）（部分個人情報の暗号化）本発明は、匿名通信路を利用することなしに、個人情報提供者の個人情報を登録する個人情報管理センタ装置においても、個人情報提供者のプライバシーが知られることがない。

【0185】（7）（全体）本発明は、個人情報提供者の個人情報を登録する個人情報管理センタ装置に個人情報提供者のプライバシーが知られるなど、個人情報提供者以外の者に個人情報提供者のプライバシーが知られることなしに、個人情報提供者が許諾した個人情報利用者が、個人情報提供者の許諾した方法で個人情報を利用するように個人情報提供者が制御することができる。また、個人情報提供者が、個人情報利用者に対し、個人情報の統計的利用のみを許諾することができる。

【図面の簡単な説明】

【図1】システムの全体構成を表す。

【図2】個人情報提供者端末装置の構成を表す。

【図3】個人情報管理センタ装置の構成を表す。

【図4】個人情報登録処理のフローを表す。

【図5】個人情報取得処理のフローを表す。

【図6】システムの全体構成を表す。

【図7】個人情報提供者端末装置の構成を表す。

【図8】個人情報管理センタ装置の構成を表す。

【図9】個人情報利用者端末装置の構成を表す。

【図10】部分個人情報DBの構成例を表す。

【図11】部分個人情報関連DBの構成例を表す。

【図12】部分個人情報識別子DBの構成例を表す。

【図13】全体的な処理の概要を表す。

【図14】個人情報登録処理のフローを表す。

【図15】個人情報提供処理のフローを表す。

【図16】個人情報取得処理のフローを表す。

【図17】入力される個人情報の例を表す。

【図18】部分個人情報への分割の一つ目の例を表す。

【図19】部分個人情報への分割の二つ目の例を表す。

【図20】部分個人情報DBへ保存されるデータの例を表す。

【図21】部分個人情報関連DBへ保存されるデータの例を表す。

【図22】個人情報変更処理のフローを表す。

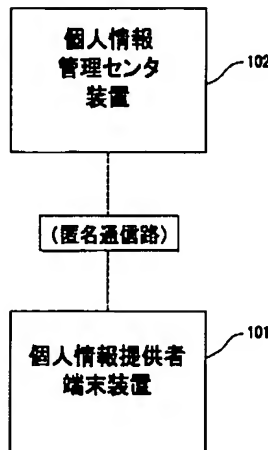
【図23】部分個人情報DBの構成例を表す。

- 【図24】部分個人情報関連DBの構成例を表す。  
 【図25】個人情報管理センタ装置の構成を表す。  
 【図26】個人情報提供処理のフローを表す。  
 【図27】個人情報取得処理のフローを表す。  
 【図28】部分個人情報利用許諾情報の構成例を表す。  
 【図29】個人情報管理センタ装置の構成を表す。  
 【図30】個人情報取得処理のフローを表す。  
 【図31】個人情報登録処理のフローを表す。  
 【図32】個人情報取得処理のフローを表す。  
 【図33】暗号化された部分個人情報の例を表す。  
 【図34】個人情報取得処理のフローを表す。  
 【符号の説明】

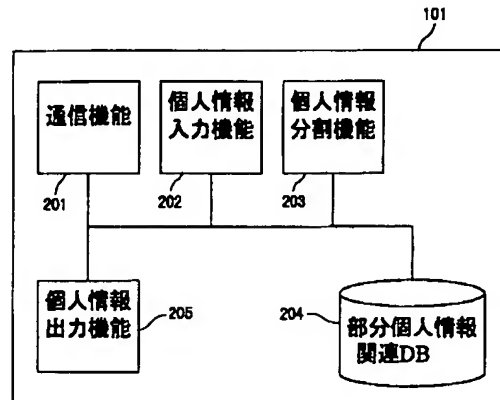
101、601…個人情報提供者端末装置

- 102、603…個人情報管理センタ装置  
 602…個人情報利用者端末装置  
 202…個人情報入力機能  
 203、703…個人情報分割機能  
 204、704…部分個人情報関連DB  
 302、802、2502、2902…部分個人情報識別子生成機能  
 303、803、2504、2905…部分個人情報DB  
 10 903…部分個人情報識別子DB  
 2503…利用条件判断機能  
 2904…部分個人情報順序入換機能

【図1】

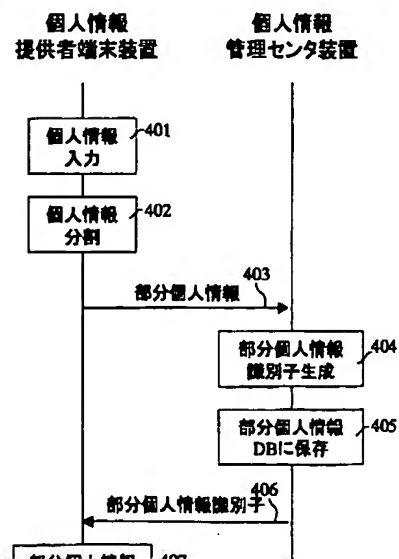
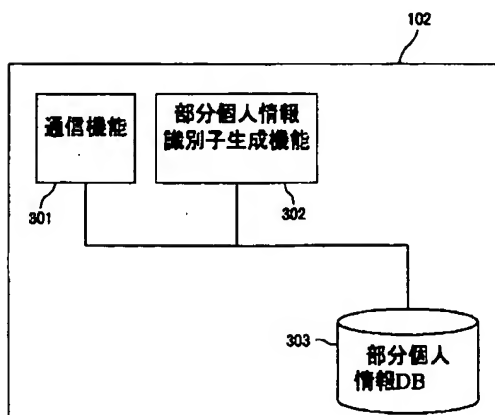


【図2】



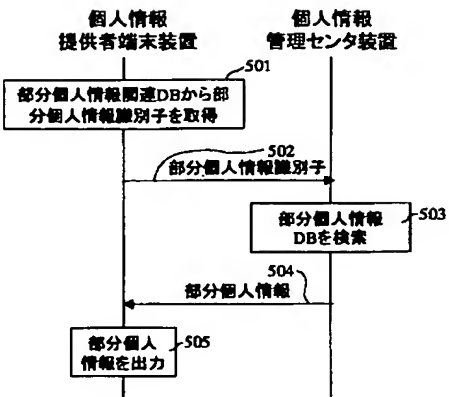
【図4】

【図3】

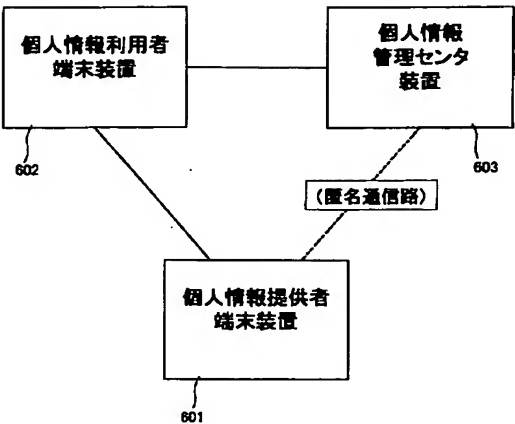




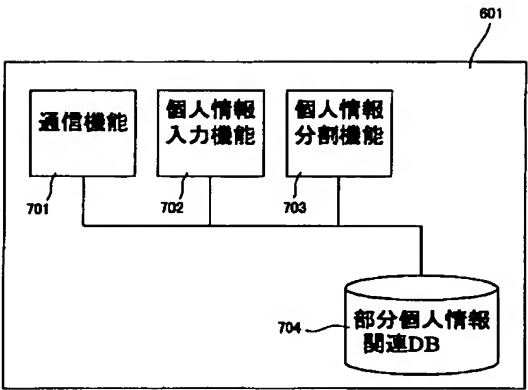
【図5】



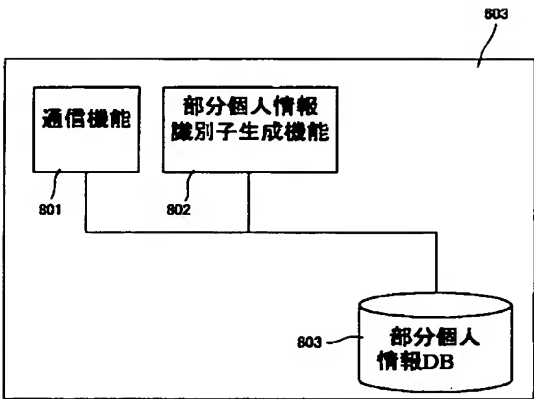
【図6】



【図7】



【図8】



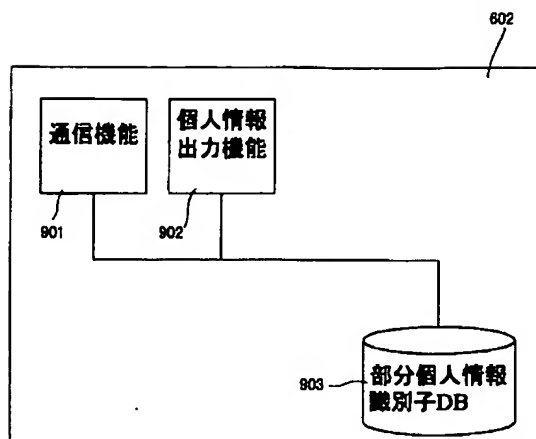
【図10】

部分個人情報識別子	部分個人情報
$id_1$	Alice
$id_2$	1-1 Southern Ave.

【図11】

部分個人情報識別子	内容
$id_1$	氏名
$id_2$	郵便番号
$id_3$	住所
$id_4$	年齢
$\vdots$	$\vdots$
$\vdots$	$\vdots$

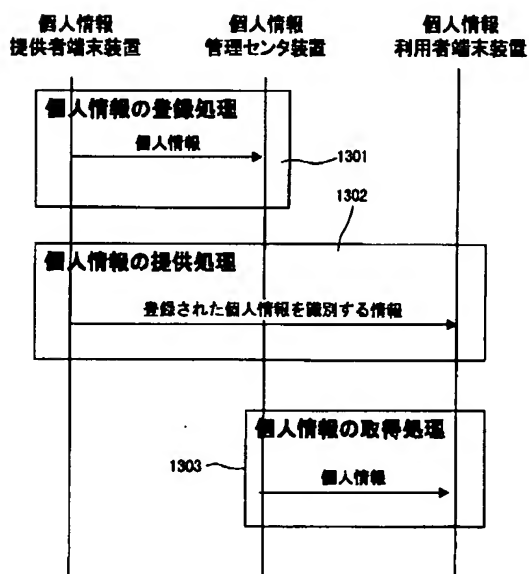
【図9】



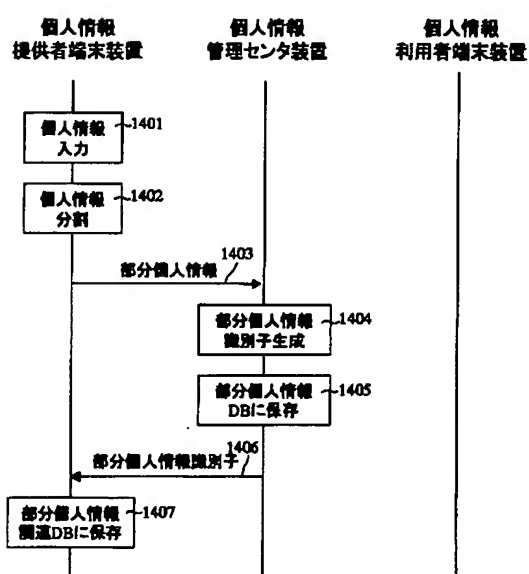
【図12】

No.	名前	趣味	...
1	$id_1$	$id_3$	
2	$id_2$	$id_4$	
:	:	:	...

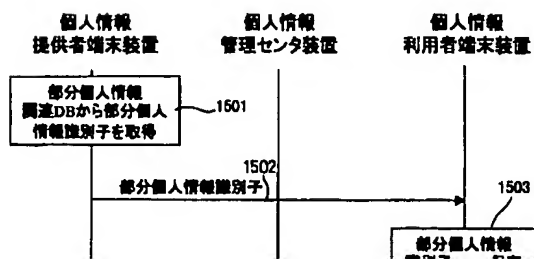
【図13】



【図14】



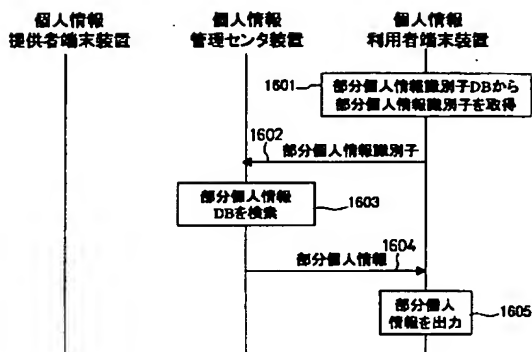
【図15】



【図17】

名前	Alice
郵便番号	111
住所	1-1 Southern Ave.
年齢	24
性別	female
趣味	music

【図16】



【図18】

部分個人情報1	Alice
部分個人情報2	111
部分個人情報3	1-1 Southern Ave.
部分個人情報4	24
部分個人情報5	female
部分個人情報6	music

【図19】

部分個人情報1	A
部分個人情報2	l
部分個人情報3	i
部分個人情報4	c
部分個人情報5	e
部分個人情報6	1
⋮	⋮

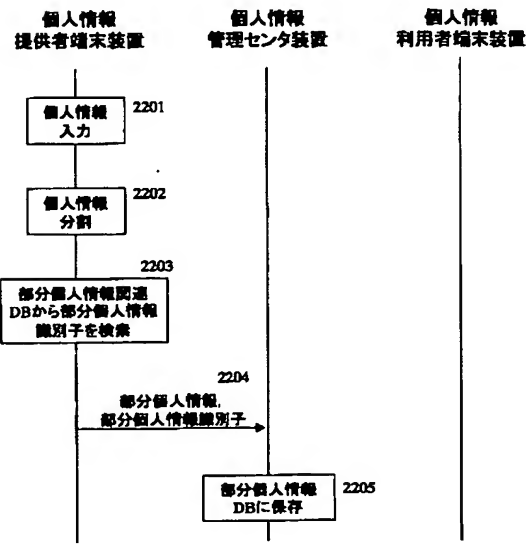
【図20】

部分個人情報識別子	部分個人情報
$id_1$	Alice
$id_2$	111
$id_3$	1-1 Southern Ave.
$id_4$	24
$id_5$	female
$id_6$	music

【図21】

部分個人情報識別子	内容
$id_1$	名前
$id_2$	郵便番号
$id_3$	住所
$id_4$	年齢
$id_5$	性別
$id_6$	趣味

【図22】



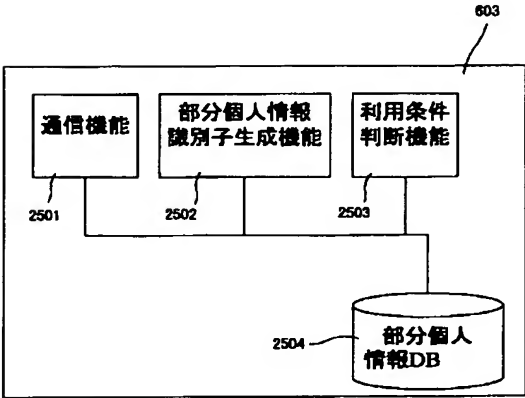
【図23】

匿名公開鍵	部分個人情報識別子	部分個人情報
Pa	id <sub>1</sub>	Alice
Pb	id <sub>2</sub>	111
Pc	id <sub>3</sub>	1-1 Southern Ave.
Pd	id <sub>4</sub>	24
⋮	⋮	⋮
⋮	⋮	⋮

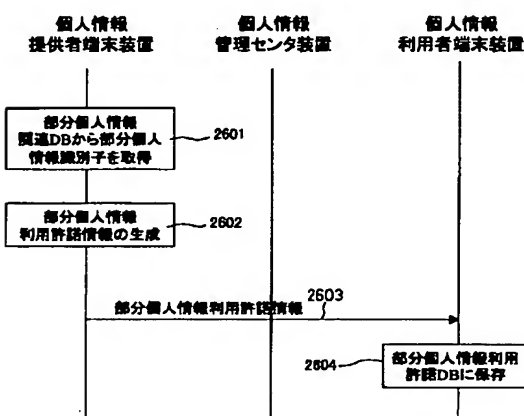
【図24】

匿名公開鍵・秘密鍵	部分個人情報識別子	内容
Pa, Sa	id <sub>1</sub>	氏名
Pb, Sb	id <sub>2</sub>	郵便番号
Pc, Sc	id <sub>3</sub>	住所
Pd, Sd	id <sub>4</sub>	年齢
⋮	⋮	⋮
⋮	⋮	⋮

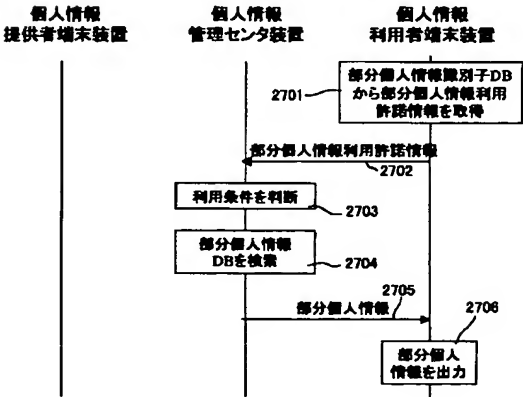
【図25】



【図26】



【図27】



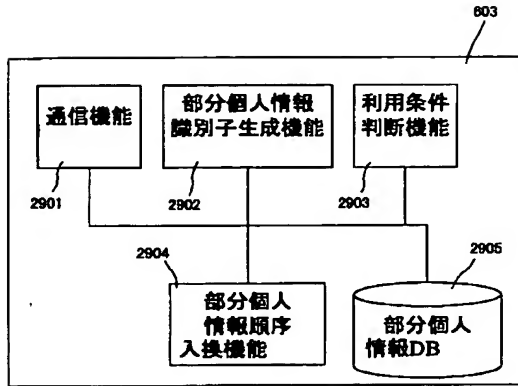
【図28】

2801	2802	2803	
個人情報利用者識別子	個人情報利用条件	部分個人情報識別子	...

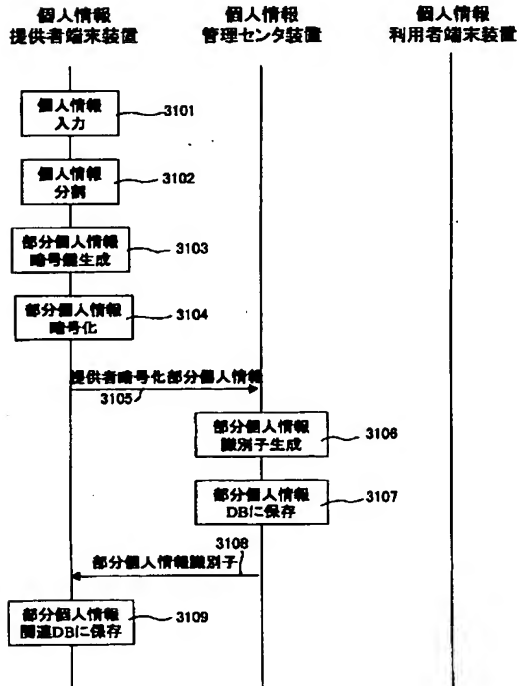
【図33】

提供者暗号化部分個人情報1	$E_{K^*}(\text{Alice})$
提供者暗号化部分個人情報2	$E_{K^*}(111)$
提供者暗号化部分個人情報3	$E_{K^*}(1-1 \text{ Southern Ave.})$
提供者暗号化部分個人情報4	$E_{K^*}(24)$
提供者暗号化部分個人情報5	$E_{K^*}(\text{female})$
提供者暗号化部分個人情報6	$E_{K^*}(\text{music})$

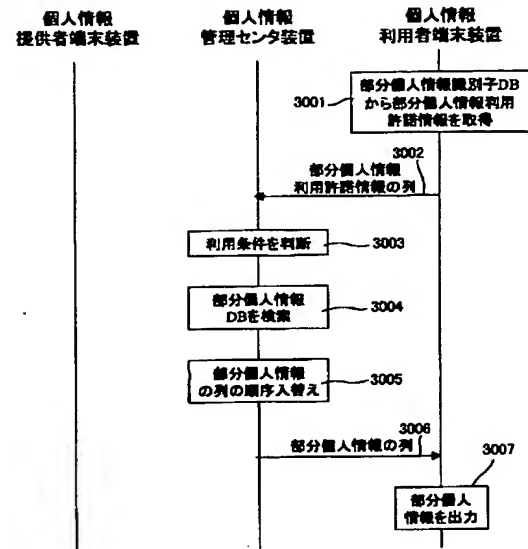
【図29】



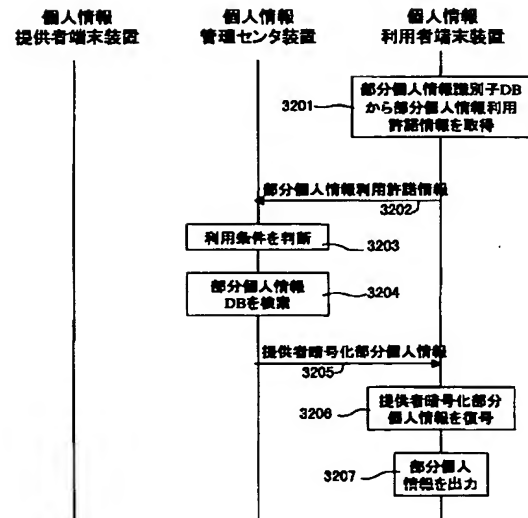
【図31】



【図30】

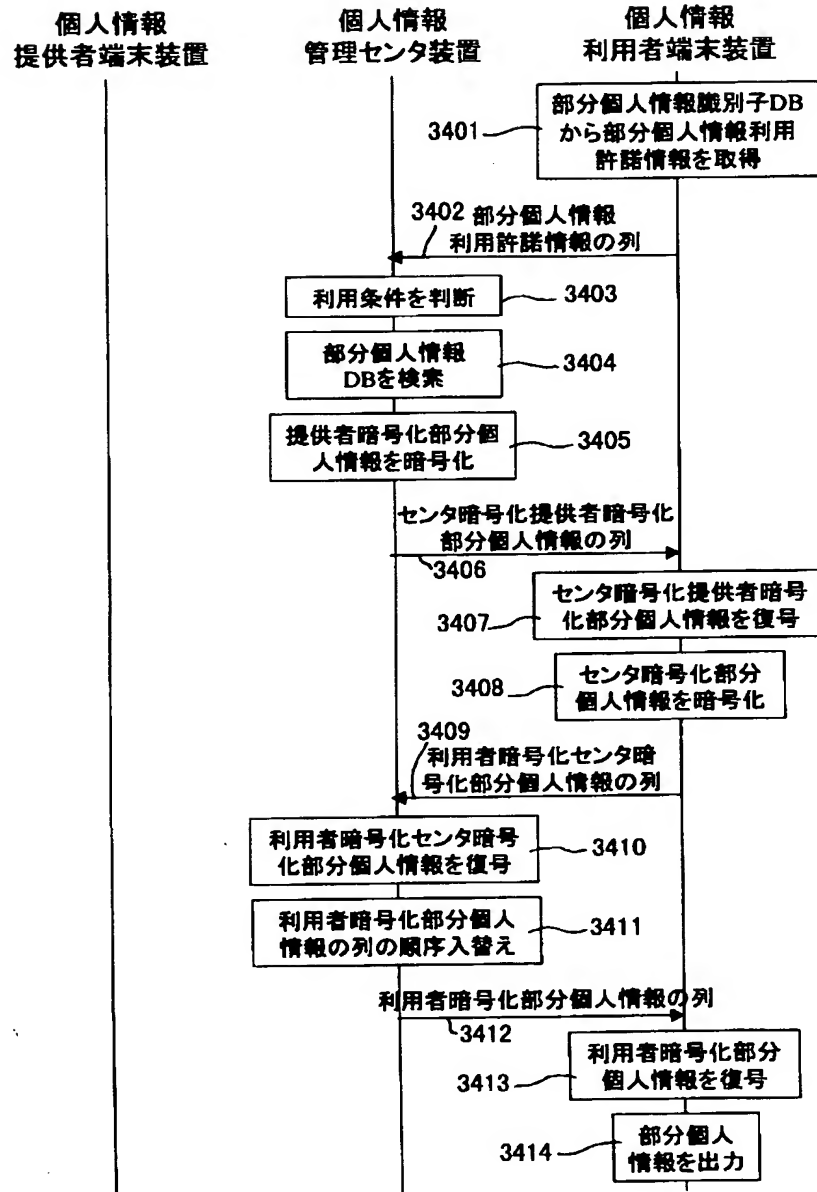


【図32】





【図34】



フロントページの続き

(51)Int.Cl.<sup>7</sup>

識別記号

F I

ターム(参考)

G 0 6 F 17/60

5 1 2

G 0 6 F 17/60

5 1 2

(72)発明者 高嶋 洋一

Fターム(参考) 5B017 AA07 BA07 BA10 BB02 CA16

東京都千代田区大手町二丁目3番1号 日

5B049 AA01 AA06 CC01 EE05

本電信電話株式会社内

5B075 KK54 KK63 ND20 UU08